Remarks

Status of application

Claims 1-64 were examined and stand rejected in view of prior art. The claims have been amended to further clarify Applicant's invention. Reexamination and reconsideration are respectfully requested.

The invention

For a summary of Applicant's invention, please refer to the annotated summary provided with Applicant's Appeal Brief, filed on 08/02/2007.

Prior art rejections

A. Section 103 rejection: Stockwell and Elliott

Claims 1-5, 7-12, 17-22, 24, 27-29, 31-33, 35-39, 45-55, 57 and 61 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Elliot (US 7,145,898 Bl). The Examiner's rejection of claim 1 is representative:

> As per claim 1, Stockwell discloses a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (fig. 1: the computers connected to internal network, col. 4 L21-42: a firewall gateway), a method for managing Internet access based on a specified access policy (col. 1 L5-10, col. 3 L16-54, col. 5 L16-22: access policies), the method comprising:
>
> a challenge/response sequence for determining whether a given client computer is in compliance with said specified access policy (col. 5 L16 to col. 6 L67, col. 9 L1-60);
>
> blocking Internet access for any client computer that does not respond appropriately to said challenge (col. 5 L16 to col. 6 L67, col. 9 L1-60: blocking the Internet access by dropping -the connection, col. II L5-67).

The Examiner acknowledges that Stockwell does not explicitly disclose the process of transmitting a challenge from the client premises equipment to each client computer and transmitting a response from at least one client computer back to the client premises equipment for responding to challenge that has been issued. However, the Examiner contends that this missing feature is provided by Elliott.

Stockwell describes a system and method for regulating the flow of internetwork connections through a firewall having a network protocol stack which includes an Internet Protocol (IP) layer. Based on the parameters characteristic of a connection request, the Stockwell system determines if authentication is required (by a corresponding rule). If authentication is required by the rule, an authentication protocol is activated and the connection is activated if the authentication protocol is completed successfully. Elliott describes a hybrid network which includes transfer of information across the Internet utilizing telephony routing information and internet protocol address information. For the portion cited by the Examiner (i.e., columns 265-266), Elliott describes the well-known logon sequence of a dial-up user for gaining Internet access (namely, the user is first authenticated based on his or her user name and password). Although it is believed that Applicant's original-filed claims distinguish over the foregoing combination, the claims have nevertheless been amended to prevent such a broad reading that the Examiner is presently according them.

At its core architectural level, Applicant's invention is fundamentally different than the combination of Stockwell with Elliott. As described in Applicant's specification, Applicant's invention includes a router-side client management protocol (CMP) installed and operational on the client's (i.e., the user's) router (client premises equipment). This operates in conjunction with a client-side security module of the present invention that is installed and running on the user's (compliant) computers. (Noncompliant computers generally will not have the security module installed.) Every few seconds the CMP component sends out a communication via Internet broadcast to connected computers that is described as a "router challenge". This router challenge -- which is repeatedly initiated by the router and not by the user or his/her computers -- requires a response from the (connected) computers within a few seconds. Computers that have the client-side security module installed and are compliant (e.g., comply with any policy required by the client-side security module) may return an appropriate response to the router challenge. Any computer that does not have the client-side security module installed or is otherwise noncompliant (i.e., fails to comply with a policy required by the client-side security module) is unable to respond to the router challenge in an appropriate manner, and thus will be blocked from Internet access by the client premises equipment (router). As should be evident at this point, Applicant's approach has the particular advantage that a given client computer must at all times be able to establish – and continue to re-establish -- its compliance with required policies. The moment a client computer fails compliance (e.g., has an out-of-date virus definition file), it is blocked from access.

Applicant's independent claims have been amended to bring these features to the forefront. For example, independent claim 1 now recites the claim limitation of (shown in amended form):

> transmitting a plurality of challenges over a period of time ~~challenge~~ from said client premises equipment to each client computer, for determining whether a given client computer ~~is~~ remains in compliance with said specified access policy during said period of time;

This claim amendment makes it clear that Applicant's invention is directed to repeatedly checking (e.g., every few seconds) the user's computers for compliance, in contrast to Elliott which (like previously-cited Fuh) simply describes a one-time user authentication (i.e., at the time of user logon). Moreover, these challenges are repeatedly transmitted from the client premises equipment (e.g., router) in a fairly autonomous manner regardless of what the client computers or user are doing -- that is, it is not predicated on some type of access request having occurred (e.g., triggering of Stockwell rule) nor does it require any sort of user action to have occurred (e.g., Elliott's user logon attempt). In this manner, Applicant's claimed invention provides around-the-clock protection of networks so that the moment that any client computer lapses into noncompliance (e.g., fails to comply with applicable corporate security policies), that computer can be effectively kicked off (i.e., denied access). Such a result is not possible with the combination of Stockwell and Elliott, as those combined references provide no teaching or suggestions for continual, router-initiated monitoring of client computers. In Applicant's approach, client computers must repeatedly and unconditionally "prove up" their compliance. In Applicant's invention, the router is constantly issuing challenges to the client computer for determining whether the client computer is in compliance with the applicable access policy governing Internet access by client computers. It is not possible to coax such a teaching from the combination of Stockwell and Elliott.

All told, the combination of Stockwell and Elliott is distinguishable from Applicant's invention on several grounds which are specifically included as claim limitations of Applicant's independent claims and other dependent claims thereof. Applicant's invention regulates Internet access by continually challenging client computers to prove that they are in compliance with applicable access policies. Therefore, as the combined art references do not teach or suggest all of the claim limitations of Applicant's independent claims (and other dependent claims thereof) it is respectfully submitted that the amended claims distinguish over this combination and overcome any rejection under Section 103.

B. Section 103 rejection: Stockwell, Elliott, and Kadyk

Claims 6 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Elliot (US 7,145,898 Bl), and further in view of Kadyk et al. (hereinafter Kadyk, US 6,996,841 B2). Here, the Examiner repeats the rejection based on Stockwell and Elliott above, but adds Kadyk for transmission of the "client hello" limitation. The claims are believed to be allowable for at least the reasons stated above pertaining to the rejection of the base claims (i.e., the parents of claims 6 and 30) on the basis of Stockwell and Elliott.

Moreover, the claims are believed to be allowable for the following additional reasons. Elliot describes user identity information (e.g., username and password) for authenticating a user. After the user's identity is authenticated, Elliot's system (like the previously-cited Fuh system) permits (at best, based on the Examiner's combination with Stockwell) particular types of network traffic initiated by that particular user. This is not Applicant's claimed approach. Applicant's approach provides for making the decision about whether or not to permit access based on a client computer's then-current compliance with any applicable access policy. The "client hello" limitation of the rejected claims of this group make it clear that Applicant's claimed approach is directed to device-to-device (i.e., router-to-computer) compliance verification irrespective of what the user is doing (including, even if the user is in fact authenticated). The combined references do not teach this limitation.

C. Section 103 rejection: Stockwell, Elliott, and Official Notice

Claims 13-16, 34, 42-44, 56 and 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Elliot (US 7,145,898 Bl), and further in view of "Official Notice". Here, the Examiner repeats the rejection based on Stockwell and Elliott, but adds Official Notice for Applicant's limitation that compliance (by which access may be granted) may be predicated on a certain application name or version (e.g., that a certain version of antivirus software be installed). The claims are believed to be allowable for at least the reasons stated above pertaining to the rejection of the base claims (i.e., parent claims 1, 24, and 45) on the basis of Stockwell and Elliott.

Moreover, the claims are believed to be allowable for the following additional reasons. As previously described, Elliot describes user identity information (e.g., username and password) for authenticating a user. After the user's identity is authenticated, Elliot's system (like the previously-cited Fuh system) permits (at best, based on the Examiner's combination with Stockwell) particular types of network traffic initiated by that particular user (i.e., based on that user's identity). This is not Applicant's claimed approach. Applicant's claimed approach, as set forth in these rejected claims, provides for determining whether or not to permit Internet access based on compliance with an access policy which specifies particular applications which are approved for Internet access. “Particular applications" in this context may mean that a certain version (namely, the current version) of antivirus software must be installed, for example. The combined references have no facility to predicate access on the basis that certain software be installed on the client computer.

D. Section 103 rejection: Stockwell, Elliott, and Shrader

Claims 23, 25, 26, 40, 41 and 62-64 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Elliot (US 7,145,898 Bl), and further in view of Shrader et al. (hereinafter Shrader, US 6,026,440). Here, the Examiner repeats the rejection based on Stockwell and Elliott, but adds Shrader for Applicant's "sandbox" limitation. The claims are believed to be allowable for at least the reasons stated above pertaining to the rejection of the base claims (i.e., parent claims 1, 24, and 45) on the basis of Stockwell and Elliott. Importantly, in these claims, the connection is redirected to a sandbox server based on noncompliance of the client computer itself (which is repeatedly tested), not on the lack of authentication of the user (Elliott) or conditional triggering of a rule based on a certain network traffic occurring (Stockwell).

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: February 29, 2008

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX